

Docket No. 50325-0631

REMARKS

The examiner is thanked for the performance of a thorough search. By this amendment, Claims 1, 4, 9, 13- 14 and 21-27 have been amended. Claim 28 has been cancelled and introduced as Claim 11. Hence, Claims 1-27 are pending in the application.

The amendments to the claims as indicated herein do not add any new matter to this application. Furthermore, amendments made to the claims as indicated herein have been made to exclusively improve readability and clarity of the claims and not for the purpose of overcoming alleged prior art. Each issue raised in the Office Action mailed September 21, 2005 is addressed hereinafter.

I. ISSUES NOT RELATING TO PRIOR ART

A. CLAIM OBJECTIONS

The following objections to claim formalities have been made: a) the numbering of the claims has skipped claim 11, jumping from claim 10 to 12, b) Claim 4 depends upon Claim 9 and as a matter of style the dependent claims should be numerically later than the claim(s) the depend upon, and c) a typographic error in Claim 27 which reads "establishing an new SSL connection."

Claim 28 has been cancelled and reintroduced as Claim 11. No new matter has been introduced by the addition of Claim 11. Therefore, the objection based on improper claim numbering has been fully addressed.

Claims 4 and 27 have been amended to correct typographical errors. Claim 4 as amended now depends from independent Claim 1 and not from Claim 9 as originally stated. Claim 27 has also been amended to correctly recite "establishing a new SSL connection". Applicant respectfully requests withdrawal of the objections to the claims.

Docket No. 50325-0631

II. ISSUES RELATING TO PRIOR ART

Claims 1-3, 5-8, 10, 14-17 and 19-26 stand rejected as being allegedly unpatentable over Applicant's admitted prior art (hereinafter referred to as "AAPA").

Claims 1-3, 5-8, 10, 14-17 and 19-26 stand rejected under 35 U.S.C. § 102(a) as being anticipated by "Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, entitled "Web Security" (hereinafter referred to as "*Stallings*").

Claims 4, 9, 18, 27 and 28 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Stallings*.

Claims 12 and 13 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Stallings* in view of USPGPUB, 2003/0046532, Gast, "System and Method of Accelerating Cryptographically Secure Sessions" (hereinafter referred to as "*Gast*").

CLAIMS 1-3, 5-8, 10, 14-17 and 19-26 ARE PATENTABLE AND "APPLICANT'S ADMITTED PRIOR ART" IS IMPROPERLY APPLIED

Claims 1-3, 5-8, 10, 14-17 and 19-26 were rejected as being unpatentable over Applicant's description of Secure Sockets Layer (SSL) as found in the Specification, paragraphs 2-7.

The Office Action contends that Claims 1-3, 5-8, 10, 14-17 and 19-26 are disclosed in AAPA. The Office Action states that Claims 1-3, 5-8, 10, 14-17 and 19-26 are rejected over Secure Sockets Layer (SSL), disclosed in the allegedly admitted prior art as found in the Specification, paragraphs 2-7. The Office Action's reliance on AAPA is improper, and the rejections are respectfully traversed.

The Office may rely upon admissions by an applicant only under extremely narrow circumstances. An admission may establish knowledge of the invention by others or public use

Docket No. 50325-0631

or sale. MPEP §706.02(c). A statement by an applicant during prosecution identifying the work of another as “prior art” is an admission that the work is available as prior art against the claims. Similarly, where the specification identifies work done by another as “prior art,” the subject matter so identified is treated as admitted prior art. *See* MPEP §2129 (citing cases). Thus, an applicant must actually admit that something is “prior art” for that something to qualify as “applicant admitted prior art.”

The Applicant has not labeled drawings in the application as “prior art.” Applicant does not use the term “prior art” to refer to anything in the application. Consequently, the application contains nothing that can properly be deemed as “applicant admitted prior art.”

Furthermore, Applicant has expressly stated in paragraph 0011, that the approaches in the background section of the Specification are not prior art to the claims in the application. Paragraph 0011 specifically states “The approaches described in this section could be pursued, but are not necessarily approaches that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, the approaches described in this section are not prior art to the claims in this application and are not admitted to be prior art by inclusion in this section.” The Office Action incorrectly interprets Applicant’s above statement to refer solely to the approach as referred to in paragraph 0009. Any reasonable reader would interpret “section” as referring to the entire Background section of the application. The statement recited in paragraph 0011 of the Specification correctly refers to all approaches described in the Background section of the Specification.

By statute, the Office is required to issue a patent on a proper application unless the Office locates prior art showing the invention. Thus, the burden of rejection based on prior art falls squarely on the Office, and the Office has the burden to find the prior art. The Office appears to rely on AAPA to avoid carrying its burden. The Office Action states “The fact that

Docket No. 50325-0631

Applicant has stated the approaches in the background of the art are not prior art, does not thereby absolve the Applicant of disclosure of other methods made by others in the past." This is a tautology; Applicant's statement does not mean that *no* prior art exists, only that Applicant's own statements in the Background are not admitted as prior art. If the Office believes that the information in the Background is prior art, then the Office must find a reference containing that information.

Thus, in light of the above arguments it is respectfully requested that the rejection based on AAPA be withdrawn.

Even if the rejection based on AAPA is proper, Claims 1-3, 5-8, 10, 14-17 and 19-26 are not anticipated by Secure Sockets Layers (SSL) as described in the Office Action.

The Office Action does not specify any statutory basis for the rejection. The Office Action does not provide the Applicant with adequate notice or reasonable particularity with respect to the statutory basis of the rejections. Instead, the Office Action merely asserts that claims 1-3, 5-8, 10, 14-17 and 19-26 are rejected over Secure Socket Layer (SSL) disclosed in AAPA. As a result, the Applicant has had to engage in guesswork to determine the statutory basis of the rejection. Applicant respectfully requests clarification as to the statutory basis of the AAPA rejection in a further non-final communication.

As best understood by the Applicant the rejections of Claims 1-3, 5-8, 10, 14-17 and 19-26 are based on 35 U.S.C. § 102. A proper anticipation rejection must show that each and every element, step or limitation of a claim is found in a single reference, in the same combination as claimed. *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628 (Fed Cir.), *cert. Den.* 484 U.S. 827 (1987).

Claims 1-3, 5-8, 10, 14-17 and 19-26 are not taught or disclosed by the Office Action's description of Secure Sockets Layers (SSL). The rejection is respectfully traversed.

Docket No. 50325-0631

Claim 1

The rejection of Claim 1 is founded on the Office Action's description of SSL as stated in the present Office Action. The Office Action's reliance on the discussion of SSL glosses over specific terms recited in the claim and relies on an over-reaching reading that is unreasonable. Claim 1 recites numerous elements that are in no way taught, suggested or disclosed by the Office Action's description of SSL.

Amended Claim 1 recites:

A method of providing data from a service to a client over a telecommunication network based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

- receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;
- determining an encryption type match by matching the list of encryption types received from the client list of encryption types to a mapping of encryption types to a list of one or more available online services**
- selecting an online service that can provide the data to the client, based on the encryption type match and the list of one or more available online services associated with the encryption type match; and**
- causing communication of the data from the selected online service to the client.

The use of SSL architecture and protocol as described in the Office Action's description of SSL does not teach, suggest or disclose one or more of the above bolded steps recited in Claim 1.

The Office Action specifically recites "First, there is a key exchange of 'handshake' phase, in which the server and client attempt to agree upon an encryption suite to be used for data transmission. After the key exchange or 'handshake' is negotiated, a bulk encryption of data transmission phase is carried out which the desired content is transmitted using the agreed-upon encryption suite." This does not disclose or suggest the various elements of Claim 1.

Docket No. 50325-0631

Specifically, the Office Action provides no support for a) a mapping of encryption types to a list of one or more available online services, b) determining an encryption type match by matching the list of encryption types received from the client list of encryption types of contained in the mapping, and c) selecting an online service based on the encryption type match and the list of one or more available online services associated with the encryption type match.

The Office Action does not provide any support for the above elements of Claim 1. For instance, the Office Action's description of SSL does not discuss a mapping of encryption types to services. The mapping is used to determine what level of encryption is required by a user requesting a particular service. For example, an administrator for an online banking service creates a mapping of online banking services, such as Modifying Account, Account Overview, etc. to various encryption levels. In some circumstances the administrator might determine that a modification of an account may require a higher level of encryption than an account overview. Therefore, in order to modify the account a user must possess at minimum this level of encryption in order to use the Modifying Account service.

Further, the description of SSL in the Office Action does not provide for determining an encryption type match by matching the list of encryption types received from the client list of encryption types contained in the mapping. Nothing in the Office Action's description of SSL suggests determining an encryption type match based on a list and a mapping. SSL merely relies on one proposed cipher suite to determine an encryption match, not a list of encryption type and a mapping of encryption types to services.

In addition, the description of SSL in the Office Action does not provide support for selecting an online service based on the encryption type match and the list of one or more available online services associated with the encryption type match. The handshake protocol of SSL is used to determine an encryption and cryptographic keys to be used to protect data sent

Docket No. 50325-0631

between a server and client. The Office Action's description of SSL does not teach, disclose or suggest selecting an online service based on the encryption type.

Because one or more elements of Claim 1 are not discussed, taught or suggested by the Office Action's description of SSL, Claim 1 is patentable over SSL. Reconsideration of the rejection is respectfully requested.

CLAIMS 1-27 ARE PATENTABLE OVER STALLINGS AND GAST

Claims 1-3, 5-8, 10, 14-17 and 19-26 are rejected under 35 U.S.C. § 102(a) as being unpatentable over *Stallings*. The rejection is respectfully traversed.

Claim 1

Stallings does not teach, suggest or disclose one or more of the elements recited in Claim 1. While both Claim 1 and *Stallings* deal with data encryption between a client and server the approaches of both are fundamentally different.

The portion of *Stallings* relied on by the Office Action describes the Handshake protocol of SSL. The handshake protocol consists of a series of message exchanges by client and server (Page 450). The SSL Handshake Protocol is illustrated in *Stallings* Page 451 Figure 14.6. There are fundamental differences between the Handshake Protocol described by *Stallings* and the elements recited in Claim 1.

Specifically, *Stallings* does not teach, suggest or describe a) a mapping of encryption types to a list of one or more available online services, b) determining an encryption type match by matching the list of encryption types received from the client to a list of encryption types contained in the mapping, c) selecting an online service based on the encryption type match and the list of one or more available online services associated with the encryption type match.

Docket No. 50325-0631

The mapping of online services to encryption types is established prior to any communication between the client and the server. For example, an administrator determines the mapping of online services to required levels of encryption. The mapping of services to encryption types determines what services, if any, a client can obtain in the approach of Claim 1. Nothing in *Stallings* discusses a mapping of online services to encryption types.

Additionally, *Stallings* does not teach or suggest the step of determining an encryption type match by matching the list of encryption types received from the client to a list of encryption types **contained in the mapping**. For example, the encryption type agreed upon between the server and the client is based on a **list of encryption types** the client possesses and **those encryption types listed in the mapping**. If a client does not possess in its list of encryption types an encryption type contain in the mapping, the client will be blocked from receiving that service.

Furthermore, *Stallings* does not provide selecting an online service based on the encryption type match and the list of one or more available online services associated with the encryption type match. In sharp contrast, *Stallings* states the handshake protocol “allows the server and client to authenticate each other and to negotiate and encryption and cryptographic keys to be used to protect data send in an SSL record. The handshake protocol is used before any application data is transmitted” (Page 450).

Thus, *Stallings* does not teach, suggest or disclose one or more of the limitations recited in Claim 1. Claim 1 is therefore patentable over *Stallings*. Reconsideration is respectfully requested

Claims 11, 27

Claims 11 (formerly Claim 28) and 27 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Stallings*.

Docket No. 50325-0631

Independent Claims 11 and 27 recite features similar to those discussed above with respect to Claim 1. Consequently, it is respectfully submitted that Claims 11 and 27 are patentable over the cited art, and are each in condition for allowance, for at least the reasons given above with respect to Claim 1.

Claim 13

Claim 13 was rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Stallings* in view of *Gast*.

Claim 13 recites features similar to those discussed above with respect to Claim 1. Specifically, Claim 13 also recites features of a particular encryption mapping. Consequently, it is respectfully submitted that *Stallings* does not teach, suggest or disclose one or more of the limitations of Claim 13 for at least the reasons given above with respect to Claims 1.

Similarly *Gast* does not disclose or suggest in any way the limitation recited in Claim 13 of "matching a cipher suite list received from the client to the mapping to result in identifying at least one cipher suite in common between the cipher suite list and the mapping." Nor does *Gast* teach the limitation of "identifying from the mapping an online service corresponding to the cipher suit in common". In fact, the Office Action has not alleged that *Gast* teaches these limitations.

As shown above *Stallings* and *Gast*, alone or in combination, fail to teach all the limitations of Claim 13. Therefore, Claim 13 is patentable over *Stallings* in view of *Gast*. Reconsideration and allowance of Claim 13 is respectfully requested.

Claims 13, 14 and 21-26

Docket No. 50325-0631

Independent Claim 13, 14 and 21-26 recites features similar to those discussed above with respect to Claim 1. Consequently, it is respectfully submitted that Claims 13, 14 and 21-26 are patentable over the cited art, and are each in condition for allowance, for at least the reasons given above with respect to Claim 1.

Remaining Dependent Claims

The remaining claims not discussed so far are dependent claims, each of which depends (directly or indirectly) on one of the claims discussed above. Each of the remaining dependent claims are therefore allowable for the reasons given above for the claim on which it depends. In addition, each of the remaining dependent claims introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case, a separate discussion of those limitations is not included at this time. The Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

III. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.


Docket No. 50325-0631

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firm check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: 28-Nov-2005


Christopher J. Palermo
Reg. No. 42,056

2055 Gateway Place Suite 550
San Jose, California 95110-1093
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on

11/29/05

by


Tracy Reynolds